Содержание

[Вопросы](#)
[Среда](#)
[Признаки](#)

Вопросы

1. Почему делает Cisco Web Security Appliance информация о CRL полосы (WSA) от генерируемых сертификатов при дешифровании Трафика HTTPS?
2. При генерации "поддельного" серверного сертификата во время расшифровки SSL WSA разделяет список отозванных сертификатов (CRL) от исходного сертификата. Почему это сделано?

Среда

WSA любая версия, прокси HTTPS и расшифровка SSL включен.

Признаки

Информация о CRL в сертификате исходного сервера больше не присутствует в генерируемом сертификате при дешифровании Трафика HTTPS на WSA, и таким образом клиенты не могут подтвердить, был ли отозван сертификат.

WSA разделяет информацию о CRL, потому что это больше не действительно для генерируемого сертификата. Пояснение включает понимание того, как работают CRL.

Центр сертификации (CA) может дополнительно вести список сертификатов, которые он считает больше не действительным, названным списком отозванных сертификатов или CRL. Сертификат может быть отозван по ряду причин - CA может решить, что объект, который запросил сертификат, не то, кто они сказали, что были, или о секретном ключе, привязанном к сертификату, можно сообщить украденный. Клиенты, которые проверяют идентичность Web-сервера на основе серверного сертификата со знаком, могут консультироваться с CRL, чтобы подтвердить, что не был отозван сертификат.

CRL содержит список сертификатов, которые были отозваны определенным CA, и тот список тогда подписан CA., Отозванные сертификаты определены серийным номером. Клиент может получить этот CRL и затем подтвердить, что серверный сертификат не перечислен в CRL. URL для загрузки CRL обычно включается как поле в сертификате. Как практический способ, большинство клиентов не проверяет сертификаты против CRL.

Когда WSA дешифрует HTTPS или трафик SSL, это делает это путем генерации нового серверного сертификата и подписания его с его собственным внутренним CA **(сертификат, загруженный, или генерируемый под HTTPS проксируют раздел)**.

Если бы WSA не разделял информацию **о CRL**, то клиент , который хотел проверить CRL, нашел бы, что **сертификат** и **CRL подписаны другими центрами сертификации**, и или игнорируют CRL или отмечают ошибку. Кроме того, при некоторых обстоятельствах, WSA изменит серийный номер в генерируемом сертификате, чтобы быть другим, чем серийный номер в исходном сертификате. Это означает, что, даже если бы клиент проигнорировал различие в CA между CRL и WSA-генерируемым сертификатом, информация о серийном номере не была бы допустима.

Лучший способ решить проблему для WSA, чтобы проверить сам CRL от имени клиента и затем исключить информацию о CRL из сертификата. WSA не способен к выполнению этого сегодня.

На версиях AsyncOS 7.7 и выше:

Начиная с Версии 7.7 AsyncOS WSA поддерживает **Онлайновый протокол статуса сертификации (OCSP)**, который является альтернативой CRL.

Когда включено, OCSP предоставляет способность получить статус аннулирования цифрового сертификата X.509.